VULNERABILITY BULLETINS

Critical Zyxel Vulnerability CVE-2023-28771

TLP:WHITE

May 01, 2023

Summary:

On May 1, 2023, Health-ISAC was made aware of a Zyxel vulnerability that could be used for remote code execution attacks.

Headquartered in Hsinchu, Taiwan, Zyxel is a global networking equipment and solutions provider that offers a wide range of products for businesses and consumers. The company specializes in developing and manufacturing network devices, including switches, routers, firewalls, wireless access points, and network storage devices. Zyxel products are used by small and medium-sized businesses, enterprise organizations, service providers, and home users across all sectors, including healthcare.

Health-ISAC has delivered Targeted Alerts to member organizations known to be leveraging Zyxel appliances for network defense.

Analysis:

The vulnerability, tracked as CVE-2023-28771, is rated 9.8 on the Common Vulnerability Scoring System (CVSS). According to Zyxel, some firewall versions display an improper error message handling that could allow an unauthenticated attacker to execute some OS commands remotely by sending crafted packets to affected devices.
Products impacted by the flaw are below:

- ATP (versions ZLD V4.60 to V5.35, patched in ZLD V5.36)
- USG FLEX (versions ZLD V4.60 to V5.35, patched in ZLD V5.36)
- VPN (versions ZLD V4.60 to V5.35, patched in ZLD V5.36), and
- ZyWALL/USG (versions ZLD V4.60 to V4.73, patched in ZLD V4.73 Patch 1)

Zyxel has addressed the vulnerability by releasing a firmware update that fixes the flaw. Zyxel also announced fixes for several high-severity flaws in multiple firewalls and access point (AP) models, which could be exploited to cause denial-of-service (DoS) conditions, execute commands, cause a core dump, or retrieve encrypted information of the administrator.

Recommendations:

Zyxel advises its customers to update their devices to the latest firmware version as soon as possible to ensure that they are protected from this vulnerability. Additionally, Zyxel recommends that customers configure their firewalls to only allow trusted users to access the device and monitor their network for any suspicious activity.

Reference(s)	The Hacker News, Security Week, cybersecuritynews, Zyxel

CVSS Score
9.8

Release Date
1682999999

Alert ID 794fa7bb

View Alert

Tags CVE-2023-28771, PaperCut, Zyxel

TLP:WHITE Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction.

For Questions or Comments

Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App.  

For more update and alerts, visit: **https://health-isac.cyware.com**

If you are not supposed to receive this email,
please contact us at **toc@h-isac.org**.